REMARKS

Claims 1 – 9 are presently pending in the application. Claims 2, 5, 7, and 8 have been amended to correct minor typos. No new matter has been added and support for the amendments to the claims can be found in the specification and drawings. In view of the above claim amendments and arguments for patentability presented hereinbelow, Applicants respectfully submit that the application is now in condition for allowance.

Claim Rejections – 35 U.S.C. § 102(e)

Claims 1, 2 and 7 stand rejected under section 102(e) as being anticipated by Forslow U.S. Patent Publication No. 2003/0039237("Forslow"). Applicants respectfully traverse this rejection and submit that Forslow fails to disclose or suggest the claimed invention.

In accordance with an aspect of the invention, a method and apparatus are provided for supporting IP networking for mobile hosts. The apparatus is an "intelligent device" that can be installed on or connected to a mobile host. The intelligent device may comprise a software-only logical module, physical hardware, or a combination of both. To a mobile host, the intelligent device emulates a network interface such as an Ethernet card or a telephone modem. The intelligent device appears to an access network just like any regular IP host connected to the access network through a physical network interface device. Accordingly, the intelligent device, instead of the operating system on the mobile host as required by Mobile IP and IPsec, handles all mobile networking functions for the mobile host. The intelligent device may control multiple different physical network interface devices to enable a connection to the "best" access network available to the mobile user at his location. Furthermore, the intelligent device can be pre-configured or remotely configured by a service provider, thereby obviating any need for a mobile user to have specialized networking knowledge in order to make the network connections.

The intelligent device can support several IP networking functions for the mobile host with which it is associated. For example, the mobile host can be connected to the Internet or it's home network via any access network so long as the access network has an agreement with the mobile host's Internet service

provider (ISP) or home network owner to provide IP connectivity to the mobile user. In this regard, the access network will assign a local IP address (called access IP address) to the mobile host, which can be used to route IP packets for the mobile host over the Internet through the access network as long as the mobile host has a connection to the access network. The access network may only allow the mobile host use this access IP address to send/receive packets to/from a gateway in its ISP network (i.e., a portion of the Internet) or home network (e.g., an intranet behind firewall).

From the mobile host's point of view, the mobile host is always "directly" and "statically" connected to its ISP or home network and always has IP connectivity. That is, the mobile host will always use an IP address that is obtained from its ISP or its home network (the home IP address). Accordingly, the mobile host (specifically, the IP stack of the operating system of the mobile host) doesn't know and doesn't need to know if the mobile user is roaming. Home IP connectivity seamlessly and transparently maintained while the mobile user roams, including moving from one access network to another. To support this feature, the intelligent device maintains an IP tunnel to a Mobile IP Home Agent (HA) or some gateway capable of mobility management in the mobile host's ISP or home network, whenever the mobile host is not directly connected to its ISP or home network.

The intelligent device monitors all physical network interfaces for available access networks to the mobile user in his current location, and automatically switches to the "best" access network based on channel quality, charging scheme, data rate, moving speed, access coverage, and user preference, etc. The switching operation is unknown to the mobile host and does not break the mobile host's IP connectivity. To perform a switch, the intelligent device needs to obtain a new access IP address from the new access network; to establish a new IP tunnel to its home agent using the new access IP address; to release the old access IP address; and to remove the old IP tunnel associated with the old access IP address.

The IP packets can be secured while they are routed in the access network. If the mobile host is connected to its home network via an access network and an

HA that doesn't belong to its home network, the IP packets can be secured while they are routed in the access network and by the HA. See Specification at pages 7 – 10.

In this regard, representative claim 1 calls for:

A method of connecting a mobile host to an access network *with an intelligent device connected to the mobile host*, comprising the steps of:

(a) *receiving a host configuration request message from the mobile host* using a host configuration protocol;

(b) *sending an access request to the access network*;

(c) *receiving a response to the access request from the access network* with an IP address for the mobile host;

(d) selecting an IP address in the same subnet as the IP address for the mobile host; and

(e) *sending a reply message to the mobile host* with the selected IP address as the source IP address and the IP address for the mobile host as the destination IP address.

Claim 1 (emphasis added).

Turning now to Forslow, that reference discloses a methodology for specifying an individual application flow between a circuit-switched network and a packet switched network depending on the desired quality of service (QoS) requested for the individual application flow. See Abstract.

The Examiner cites to Forslow for the teachings of:

> ...a method of connecting a mobile station to a network (see [0051]). The method includes assigning an IP address to the mobile station (see [0051]). Forslow further teaches a request to access a network using a configuration protocol DHCP, the IP assignment includes assigning an IP address corresponding to a common subnet mask and sending a reply message to the mobile station (see [0101-0102]). The method further includes using the IP address as the source address for sending data between the network ISP and the mobile device (see [0051]).

Office Action at page 3.

It is axiomatic that in order to support a proper Section 102 rejection, every element in the claim must be found in the cited reference. Applicants submit that Forslow fails to support a proper section 102 rejection as several elements found in claim 1 are not disclosed in the cited reference, and further that Forslow fails to suggest the claimed invention.

In Applicants' system, an intelligent device is coupled to the mobile host and appears to an access network just like any regular IP host connected to the access network through a physical network interface device. Accordingly, the intelligent device, instead of the operating system on the mobile host, handles all mobile networking functions for the mobile host. In this connection, Claim 1 calls for "[a] method of connecting a mobile host to an access network with *an intelligent device connected to the mobile host*" which receives "a host configuration request message *from the mobile host* using a host configuration protocol"; sends "an access request *to the access network*"; receives "a response to the access request from the access network with an IP address for the mobile host"; selects "an IP address *in the same subnet as the IP address for the mobile host*"; and sends "a reply message *to the mobile host with the selected IP address as the source IP address and the IP address for the mobile host as the destination IP address*." This arrangement is neither disclosed nor suggested by Forslow.

By way of contrast, in the cited portions of Forslow, an arrangement is described where *the mobile host itself* handles the networking functions as clearly stated in the description. For example, "[a]fter PDP context activation, a network layer, e.g., IP, host configuration operation is performed to establish a network (IP) bearer communication between the mobile host and an external network entity like an ISP. The IP configuration includes assigning a network layer (IP) address to the mobile station...." See Forslow at ¶0051. The cited portions at ¶0101-0102 merely describe a configuration relay agent 120 that is disposed in the network to relay DHCP messages between the DHCP client in the mobile station and the DHCP server in the network. See ¶0079. This is not the same thing as an intelligent device which connects the mobile host to the network. Accordingly, it is respectfully submitted that Forslow fails to anticipate the

invention and further, that there is nothing in Forslow which suggests the claimed arrangement.

In view of the above, it is respectfully submitted that independent claim 1 is patentable over Forslow, and that those claims that ultimately dependent on claim 1 are also patentable for at least the same reasons. It is further submitted that independent claims 2 and 7 are patentable for the same reasons, and that those claims dependent on claim 2 are patentable for at least the same reasons.

The Examiner has indicated that claim 9 would be allowable. For some reason, no mention of claim 8 appears in the Office Action. Nevertheless, Applicants submit that claim 8 would be allowable for the same reasons set forth above.

Claim Rejections – 35 U.S.C. § 112

Claims 8 and 9 stand rejected under Section 112, first paragraph, as failing to comply with the enablement requirement with regard to the term "fake ARP reply." Applicants respectfully traverse this rejection and submit that the specification fully explains the term "fake ARP reply."

As set forth above, an aspect of the present invention utilizes an intelligent device installed on or connected to the mobile host. As explained in several places in the specification, "fake" messages are generated by the intelligent device which, are described as follows. See for example, the discussion in the specification on page 17, lines 3 – 14:

> The intelligent device 302 selects an IP address $IP_{DHCP@CDPD}$ which belongs to the same subnet as $IP_{MH@CDPD}$. $IP_{DHCP@CDPD}$ is used as the source IP address in a "faked" DHCP_OFFER message to the MH 300. The intelligent device 302 then packages the DHCP_OFFER message into an Ethernet frame with MAC 1 as the source MAC address and MAC 2 as the destination MAC address, and sends the frame to the MH 300 at 312. The emulated Ethernet device will cause a hardware to interruption to notify the operating system of the MH 300. The MH 300 accepts the "faked" DHCP_OFFER message from the intelligent device 302, and then sends a DHCP_REQUEST message back to the intelligent device 302 at 314. This message uses $IP_{MH@CDPD}$ as the source IP address and the "faked" $IP_{DHCP@CDPD}$ as the destination IP address.

Similarly, the specification at page 24, line 15 – page 25, line 1, contains the following description:

> The MH 900 is assumed to be within the coverage of a foreign WLAN. At 908, the MH 900 sends an ARP request to the intelligent device 902 with a source MAC address MAC 1 and the destination MAC address $MAC_{broadcast}$. The message is packaged into an Ethernet frame as described above. If no reply message is received within a specified period of time, the MH 900 assumes the link has been broken. After the intelligent device 902 receives this message, it sends *a fake ARP reply message at 910 to the MH 900 with* $IP_{DST@ON}$ *corresponding to MAC 2 as the source IP address.* At 912, the MH 900 then packages an IP packet into an Ethernet frame with MAC 1 as the source MAC address and MAC 2 as the destination MAC address, and $IP_{MH@ON}$ as the source IP address and $IP_{DST@ON}$ as the destination IP address.

Thus, Applicants respectfully disagree that the term "fake ARP reply" is not properly enabled by the specification. The description clearly states that the intelligent device sends a "fake" ARP reply message to the mobile host with $IP_{DST@ON}$ corresponding to MAC 2 as the source IP address.

In view of the foregoing, Applicants respectfully submit that claims 1 – 9 are patentable over the cited art and allowance of these claims at an early date is solicited.

The Office is hereby authorized to charge any additional fees or credit any overpayments under 37 C.F.R. 1.16 or 1.17 to AT&T Corp. Account No. 01-2745. The Examiner is invited to contact the undersigned at (908) 707-1573 to discuss any matter concerning this application.

Respectfully submitted,
Paul Shala Henry, et al.
By:

Date:

Robert T. Canavan
Registration No. 37,592
Attorney for Applicant

FOR GHM

Canavan & Monka, LLC.
250 State Route 28, Suite 207
Bridgewater, New Jersey 08807
(908) 707-1573